

IN THE CLAIMS:

Please amend claims 1-3, 5, 7-11, 14-16, 18, 19, 21, 22, 24-29, 31, 33, 35, 36, 38, 40, 43, and 46-48 as follows. Please cancel claims 44 and 45 without prejudice or disclaimer.

1. (Currently Amended) A security server for use in a telecommunications network, the security server configured to:

receive a message;

determine whether the message is ~~from a known source or an unknown source~~ has been through a security check; ~~and, depending on a result of the determination, modify the message~~; and

forward the message within the telecommunications network regardless of the result of the determination, but if the result of the determination is that the message has not been through a security check modify the message so as to indicate that the message has not been through a security check.

2. (Currently Amended) A security server according to claim 1, wherein the security server is configured to receive a message from outside the telecommunications network.

3. (Currently Amended) A security server according to claim 1, wherein the security server is configured to modify the message so as to indicate that the message has not been through a security check by adding a parameter to the message that indicates that the message has not been through a security check ~~come from a known or an unknown source.~~

4. (Original) A security server according to claim 3, wherein the security server is configured to receive a message that includes an identity header and is further configured to add the parameter to the identity header of the message.

5. (Currently Amended) A security server according to claim 4, wherein the message comprises a session initiation protocol SIP message.

6. (Original) A security server according to claim 4, wherein the identity header comprises a P-Asserted-Identity.

7. (Currently Amended) A security server according to claim 1, configured to receive a message that includes an identity header and is further configured to modify the message so as to indicate that the message has not been through a security check by removing at least part of the identity header.

8. (Currently Amended) A security server according to claim 7, wherein the security server is configured to detect whether the identity header is of a particular type and if so to remove at least part of the header.

9. (Currently Amended) A security server according to claim 7, wherein the message comprises a session initiation protocol SIP message.

10. (Currently Amended) A security server according to claim 8, wherein the security server is configured to detect whether the identity header comprises a P-Asserted-Identity type.

11. (Currently Amended) A security server according to claim 1, wherein the security server is configured to determine whether the message ~~is from a known source or an unknown source~~ has been through a security check by determining whether or not the message has been received via a secure means.

12. (Original) A security server according to claim 11, wherein the secure means is a Za interface.

13. (Original) A security server according to claim 1, wherein the security server comprises an interrogating call session control function.

14. (Currently Amended) A network processing element for use in a telecommunications network, the network processing element configured to:

receive a message from another network element;

determine whether the message has been modified to indicate that it has not been through a security check and, ~~depending on a result of the determination, if it has been so modified,~~ perform one or more security checks in respect of the message.

15. (Currently Amended) A network processing element according to claim 14, wherein the network processing element is configured to determine whether an identity header of the message has been modified to indicate that it has not been through a security check by detecting whether the identity header of the message includes an added parameter.

16. (Currently Amended) A network processing element according to claim 15, wherein the message comprises a session initiation protocol ~~SIP~~ message.

17. (Original) A network processing element according to claim 15, wherein the identity header comprises a P-Asserted-Identity.

18. (Currently Amended) A network processing element according to claim 14, wherein the network processing element is configured to determine whether the message has been modified to indicate that it has not been through a security check by determining whether all or part an identity header of the message has been removed.

19. (Currently Amended) A network processing element according to claim 18, wherein the message comprises a session initiation protocol SIP message.

20. (Original) A network processing element according to claim 18, wherein the identity header comprises a P-Asserted-Identity.

21. (Currently Amended) A network processing element according to claim 14, ~~that comprises~~ the network processing element comprising a serving call session control function.

22. (Currently Amended) A telecommunications network comprising:
a security server; and
a network processing element,
the security server being configured to[[:]]
receive a message;

determine whether the message is ~~from a known source or an unknown source and~~, has been through a security check;

~~depending on a result of the determination~~, if the result of the determination is that the message has not been through a security check modify the message so as to indicate that the message has not been through a security check; and

forward the message to the network processing element regardless of the result of the determination.

23. (Original) A telecommunications network according to claim 22, wherein the security server is configured to receive a message from outside the telecommunications network.

24. (Currently Amended) A telecommunications network according to claim 22, wherein the network processing element is configured to:

receive a message forwarded by the security server; and

determine whether the message has been modified so as to indicate that it has not been through a security check, and, ~~depending on the result of the determination~~, if it has been so modified, perform one or more security checks in respect of the message.

25. (Currently Amended) A method of performing a security check on a message in a telecommunications network, the method comprising ~~the steps of~~:

receiving a message that has not been through a security check;

determining ~~whether~~ that the message is ~~from a known source or an unknown source~~ has not been through a security check; and, ~~depending on a result of the determination, modifying the message~~;

modifying the message so as to indicate that the message has not been through a security check; and

forwarding the message within the telecommunications network.

26. (Currently Amended) A security server for use in a telecommunications network, the security server configured to:

receive a message;

determine whether the message is ~~from a known source or an unknown source~~ has been through a security check; and

forward the message within the communications network regardless of the result of the determination but, if the result of the determination is that the message has not been through a security check, forward the message in a manner dependent on a result of the determination that indicates that the message has not been through a security check.

27. (Currently Amended) A security server according to claim 26, wherein the security server is configured to receive the message from outside the telecommunications network.

28. (Currently Amended) A security server according to claim 26, wherein the security server is configured to forward the message without security, if it is determined that the message has not been through a security check ~~is from an unknown source~~.

29. (Currently Amended) A security server according to claim 26, wherein the security server is configured to forward the message with security, if it is determined that the message has been through a security check ~~is from a known source~~.

30. (Original) A security server according to claim 28, wherein the security comprises a Zb interface.

31. (Currently Amended) A security server according to claim 26, wherein the message comprises a session initiation protocol SIP message.

32. (Original) A security server according to claim 26, wherein the security server comprises an interrogating call session control function.

33. (Currently Amended) A telecommunications network comprising:
a security server; and
a network processing element,

the security server being configured to~~[[:]]~~

receive a message;

determine whether the message has been through a security check ~~is from a known source or an unknown source~~; and

forward the message to the network processing element regardless of the result of the determination, but, if the result of the determination is that the message has not been through a security check, forward the message in a manner that indicates that the message has not been through a security check ~~dependent on a result of the determination.~~

34. (Original) A telecommunications network according to claim 33, wherein the security server is configured to receive a message from outside the telecommunications network.

35. (Currently Amended) The telecommunications network according to claim 33, further comprising: an internal security system,

wherein the security server is ~~arranged~~ configured to forward the message via the internal security system, if it is determined that ~~a~~ the message ~~is from a known source, has been through a security check, and~~

wherein the security system is configured to not forward the message via the internal security system, if it is determined that the message ~~is from an unknown source~~ has not been through a security check.

36. (Currently Amended) A telecommunications network according to claim 35, wherein the internal security system comprises a universal mobile telecommunications system ~~UMTS~~ specified security system.

37. (Original) A telecommunications network according to claim 35, wherein the internal security system comprises a Zb interface.

38. (Currently Amended) A telecommunications network according to claim 33, wherein the message comprises a session initiation protocol ~~SIP~~ message.

39. (Original) A telecommunications network according to claim 33, wherein the security server is configured to determine whether a message ~~is from a known source or an unknown source~~ has been through a security check by determining whether or not the message has been received via a secure means.

40. (Currently Amended) A telecommunications network according to claim 39, wherein the secure means comprises a universal mobile telecommunications system UMTS standard security means.

41. (Original) A telecommunications network according to claim 39, wherein the secure means comprises a Za interface.

42. (Original) A telecommunications network according to claim 33, wherein the security server comprises an interrogating call session control function.

43. (Currently Amended) A method of performing a security check on a message in a telecommunications network, the method comprising ~~the steps of:~~

receiving a message that has not been through a security check;

determining ~~whether that~~ the message ~~is from a known source or an unknown source~~ has not been through a security check; and

forwarding the message within the communications network in a manner ~~dependent on a result of the determination~~ that indicates that the message has not been through a security check.

Claims 44-45 (Canceled).

46. (Currently Amended) A security server for use in a telecommunications network, the security server comprising:

receiving means for receiving a message;

determining means for determining whether the message ~~is from a known source or an unknown source~~ has been through a security check;

modifying means for, if the message is determined not to have been through a security check, modifying the message to indicate that it has not been through a security check; and, ~~depending on a result of the determination, modify the message~~; and

forwarding means for forwarding the message within the telecommunications network regardless of whether the message has been through a security check.

47. (Currently Amended) A network processing element for use in a telecommunications network, the network processing element comprising:

receiving means for receiving a message from another network element;

determining means for determining whether the message has been modified to indicate it has not been through a security check and, ~~depending on a result of the determination~~, if it has been so modified, performing one or more security checks in respect of the message.

48. (Currently Amended) A security server for use in a telecommunications network, the security server comprising:

receiving means for receiving a message;

determining means for determining whether the message is ~~from a known source~~
~~or an unknown source~~ has been through a security check; and

forwarding means for forwarding the message within the communications network
regardless of the result of the determination but, if the result of the determination is that
the message has not been through a security check, forwarding the message in a manner
~~dependent on a result of the determination~~ that indicates that the message has not been
through a security check.